

Antonio_Valverde_Soto_SAD_UT0_

T2



Índice

Enunciado de la tarea.....	3
Ejercicio 1.....	5
Ejercicio 2.....	8
Ejercicio 3.....	11
Nessus en Windows.....	11
Nessus en Linux.....	20

Enunciado de la tarea

1. Instalación de Lynis (Linux)

Abre una terminal en el sistema Linux.

Actualiza los repositorios del sistema:

```
sudo apt update
```

Instala Lynis:

<https://cisofy.com/lynis/>

Ejecuta Lynis para realizar una auditoría completa del sistema:

El comando generará un informe con varias recomendaciones de seguridad. Guarda el informe en un archivo para su análisis.

2. Instalación de CLARA (Windows)

Descarga CLARA desde el siguiente enlace: <https://www.ccn-cert.cni.es/soluciones-seguridad/clara.html>

Descomprime el archivo descargado e instala la herramienta en tu sistema Windows.

Ejecuta CLARA y realiza una auditoría completa del sistema.

Guarda el informe de CLARA en un archivo.

3. Instalación de Nessus (Linux/Windows)

Descarga Nessus desde el siguiente enlace: <https://es-la.tenable.com/>

Selecciona la versión de prueba gratuita de Nessus.

Sigue las instrucciones de instalación para tu sistema operativo (puede ser tanto en Linux como en Windows).

Una vez instalado, abre Nessus desde el navegador web, donde te pedirá registrar una cuenta.

Configura y realiza un escaneo de vulnerabilidades en los mismos sistemas donde ejecutaste Lynis y CLARA.

Guarda los informes de los resultados.

4. Documentación de la práctica

El documento que debes entregar deberá incluir lo siguiente:

Descripción de las herramientas: Explicar brevemente para qué sirve cada herramienta y en qué sistemas se utiliza (Lynis para Linux, CLARA para Windows, Nessus para ambos).

Proceso de instalación: Instrucciones para la instalación de cada una de las herramientas.

Ejecución de los análisis: Capturas de pantalla y descripciones de los resultados obtenidos en cada sistema (informe de Lynis, CLARA y Nessus).

Propuestas de solución: Tres acciones correctivas que llevarías a cabo en base a los informes obtenidos por cada herramienta. Describir brevemente cada problema detectado y cómo planeas solucionarlo.

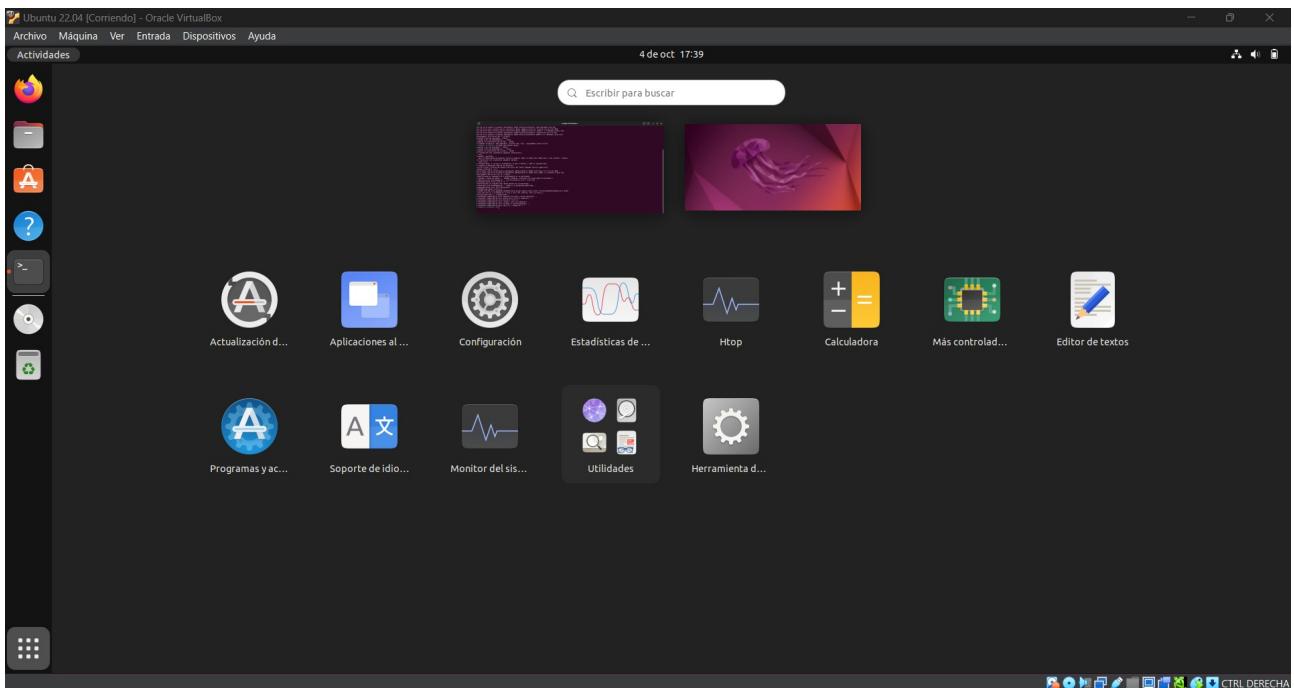
Ejercicio 1

```
toni@toni-VirtualBox:~$ sudo apt update
[sudo] contraseña para toni:
Objs:1 http://es.archive.ubuntu.com/ubuntu jammy InRelease
Des:2 http://es.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Des:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Obj:4 http://es.archive.ubuntu.com/ubuntu jammy-backports InRelease
Des:5 http://es.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [1,385 kB]
Des:6 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1,848 kB]
Des:7 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [2,067 kB]
Des:8 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [546 kB]
Des:9 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [17,9 kB]
Des:10 http://es.archive.ubuntu.com/ubuntu jammy-updates/universe i386 Translation-en [204 kB]
Des:11 http://es.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [26,3 kB]
Des:12 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [2 kB]
Des:13 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [13,3 kB]
Des:14 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [999 kB]
Des:15 http://es.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1,130 kB]
Des:16 http://security.ubuntu.com/ubuntu jammy-security/universe i386 Packages [631 kB]
Des:17 http://es.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [204 kB]
Des:18 http://es.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [26,3 kB]
Des:19 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [179 kB]
Des:20 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [19,4 kB]
Descargados 10,0 MiB en 46s (216 kB/s)
Leyendo lista de paquetes... Hecho
Creado árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 309 paquetes. Ejecute «apt list --upgradable» para verlos.
toni@toni-VirtualBox:~$
```

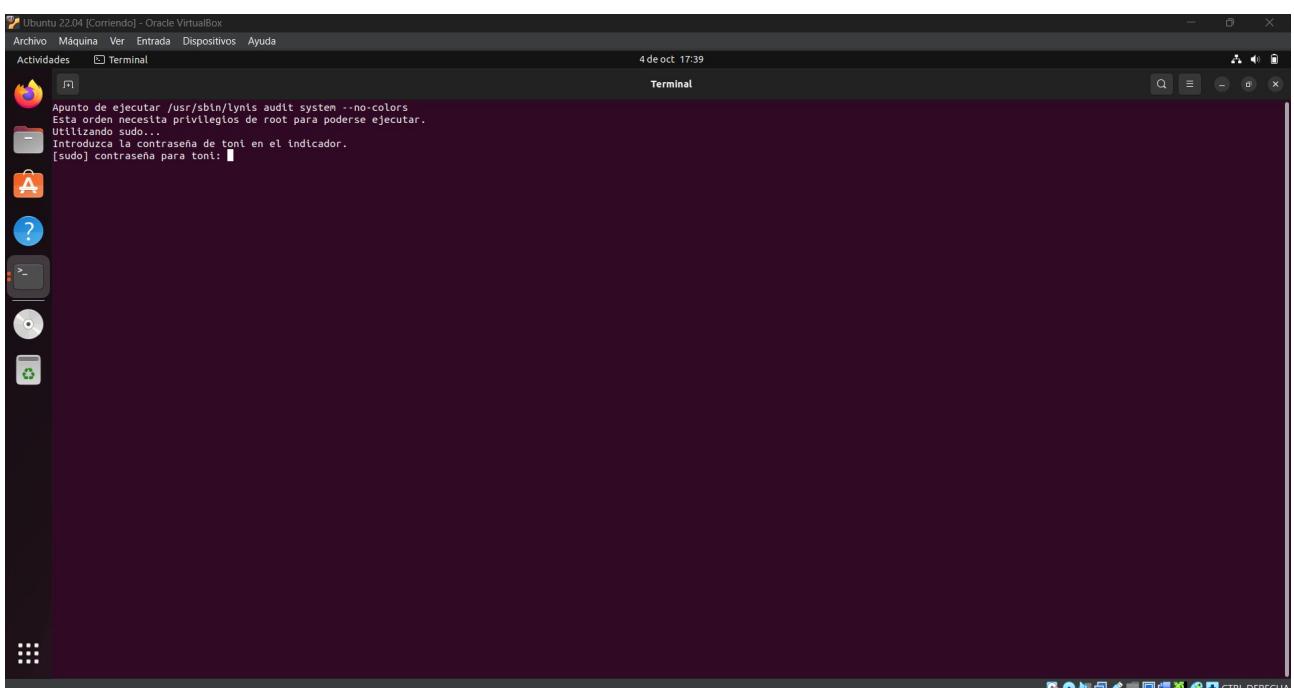
Primero actualizamos los repositorios de Ubuntu. Con el comando sudo apt update.

```
toni@toni-VirtualBox:~$ sudo apt install lynis
[sudo] contraseña para toni:
Objs:1 http://security.ubuntu.com/ubuntu jammy-security/universe i386 Packages [631 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [264 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [26,3 kB]
Des:4 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [179 kB]
Des:5 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [19,4 kB]
Descargados 10,0 MiB en 46s (216 kB/s)
Leyendo lista de paquetes... Hecho
Creado árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 309 paquetes. Ejecute «apt list --upgradable» para verlos.
toni@toni-VirtualBox:~$ sudo apt install lynis
Leyendo lista de paquetes... Hecho
Creado árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
nmap
Paquetes sugeridos:
apt-listbugs debsecan debsums tripwire samhain aide fail2ban menu-l10n_gksu | kde-runtime | ktsuss
Se instalarán los siguientes paquetes NUEVOS:
lynis
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 309 no actualizados.
Se necesita descargar 881 kB de archivos.
Después de la descarga habrá 1,08 kB espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
Des:1 http://es.archive.ubuntu.com/ubuntu jammy/universe amd64 lynis all 3.0.7-1 [227 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu jammy/universe amd64 menu amd64 2.1.47ubuntu4 [354 kB]
Descargados 581 kB en 11s (51,3 kB/s)
Seleccionando el paquete lynis previamente no seleccionado.
(Leyendo la base de datos... 183306 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../menu 2.1.47ubuntu4_amd64.deb ...
Desempaquetando menu (2.1.47ubuntu4) ...
Configurando lynis (3.0.7-1) ...
Created symlink /etc/systemd/system/timers.target.wants/lynis.timer → /lib/systemd/system/lynis.timer.
lynis.timer: Failed to start static unit not running, not starting it.
Configurando menu (2.1.47ubuntu4) ...
Procesando disparadores para desktop-file-utils (0.26-tubuntu3) ...
Procesando disparadores para gnome-menus (3.36.0-1ubuntu3) ...
Procesando disparadores para man-db (2.10.2-1) ...
Procesando disparadores para install-info (0.8-4build1) ...
Procesando disparadores para mailcap (3.70+mmu1ubuntu1) ...
Procesando disparadores para menu (2.1.47ubuntu4) ...
toni@toni-VirtualBox:~$
```

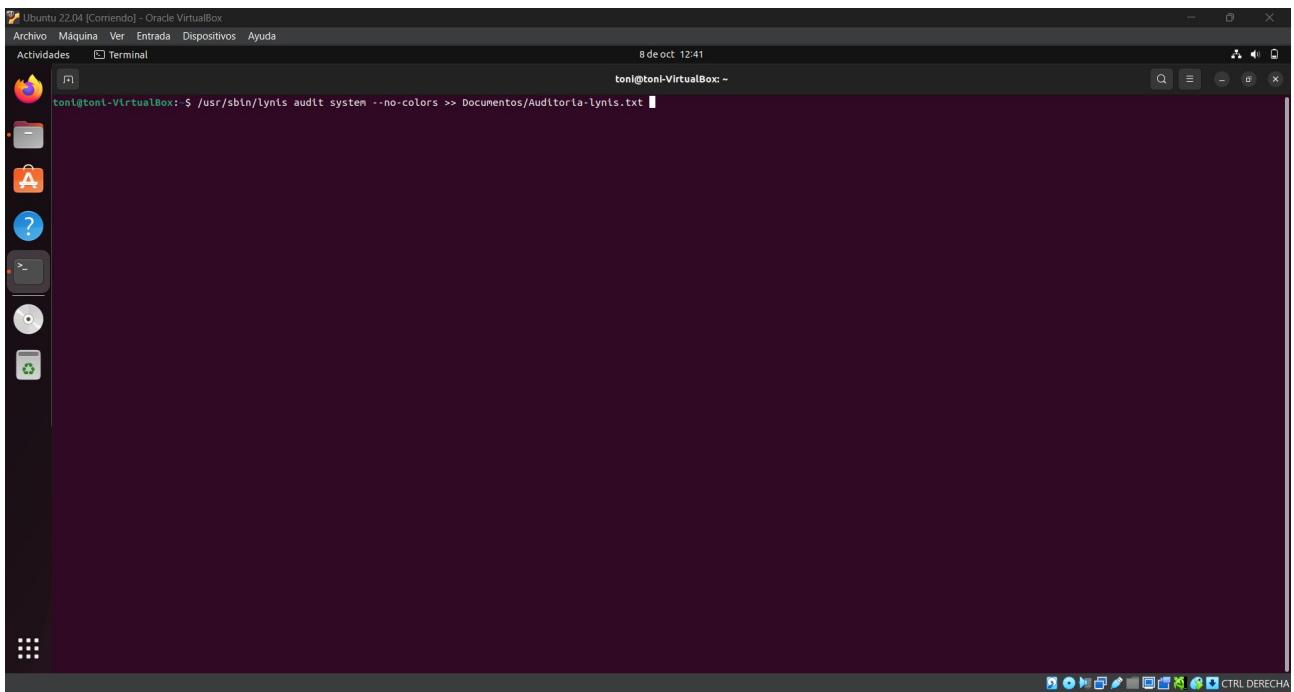
Ahora instalamos Lynis, para ello usamos el comando sudo apt install lynis.



Una vez terminado, nos aparece una nueva aplicación, llamada “Herramienta de Auditoría Lynis”.



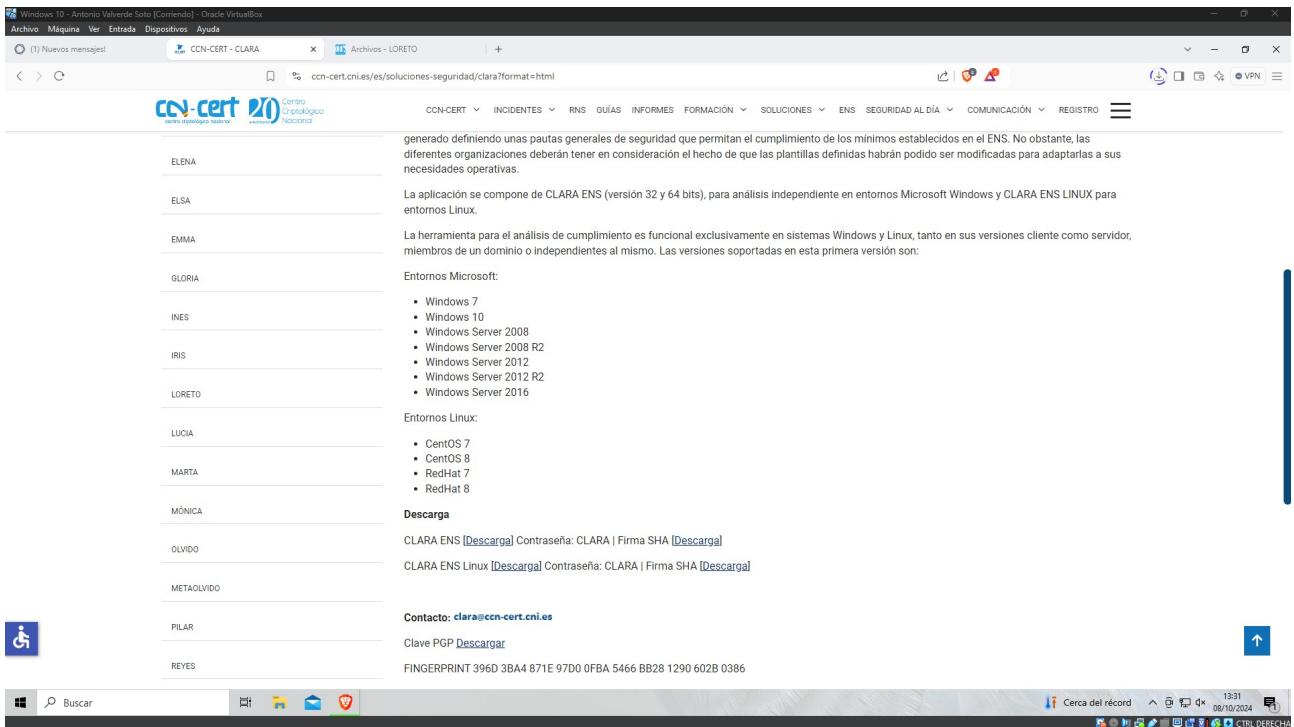
Al ejecutarlo, nos aparece lo siguiente, el comando que se va a ejecutar y nos pide poner la contraseña para ejecutarlo con privilegios de administrador, pero si lo ejecutamos así, una vez terminada la autoría nos va a cerrar la terminal.



Usando este comando que es el mismo que se ejecuta con el programa instalado, le pongo que se mande todo a un fichero, llamado Auditoría-lynis.txt.

[Pulsa aquí para ver el resultado a de la Autoría.](#)

Ejercicio 2



generado definiendo unas pautas generales de seguridad que permitan el cumplimiento de los mínimos establecidos en el ENS. No obstante, las diferentes organizaciones deberán tener en consideración el hecho de que las plantillas definidas habrán podido ser modificadas para adaptarlas a sus necesidades operativas.

La aplicación se compone de CLARA ENS (versión 32 y 64 bits), para análisis independiente en entornos Microsoft Windows y CLARA ENS LINUX para entornos Linux.

La herramienta para el análisis de cumplimiento es funcional exclusivamente en sistemas Windows y Linux, tanto en sus versiones cliente como servidor, miembros de un dominio o independientes al mismo. Las versiones soportadas en esta primera versión son:

Entornos Microsoft:

- Windows 7
- Windows 10
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Entornos Linux:

- CentOS 7
- CentOS 8
- RedHat 7
- RedHat 8

Descarga

CLARA ENS [\[Descarga\]](#) Contraseña: CLARA | Firma SHA [\[Descarga\]](#)

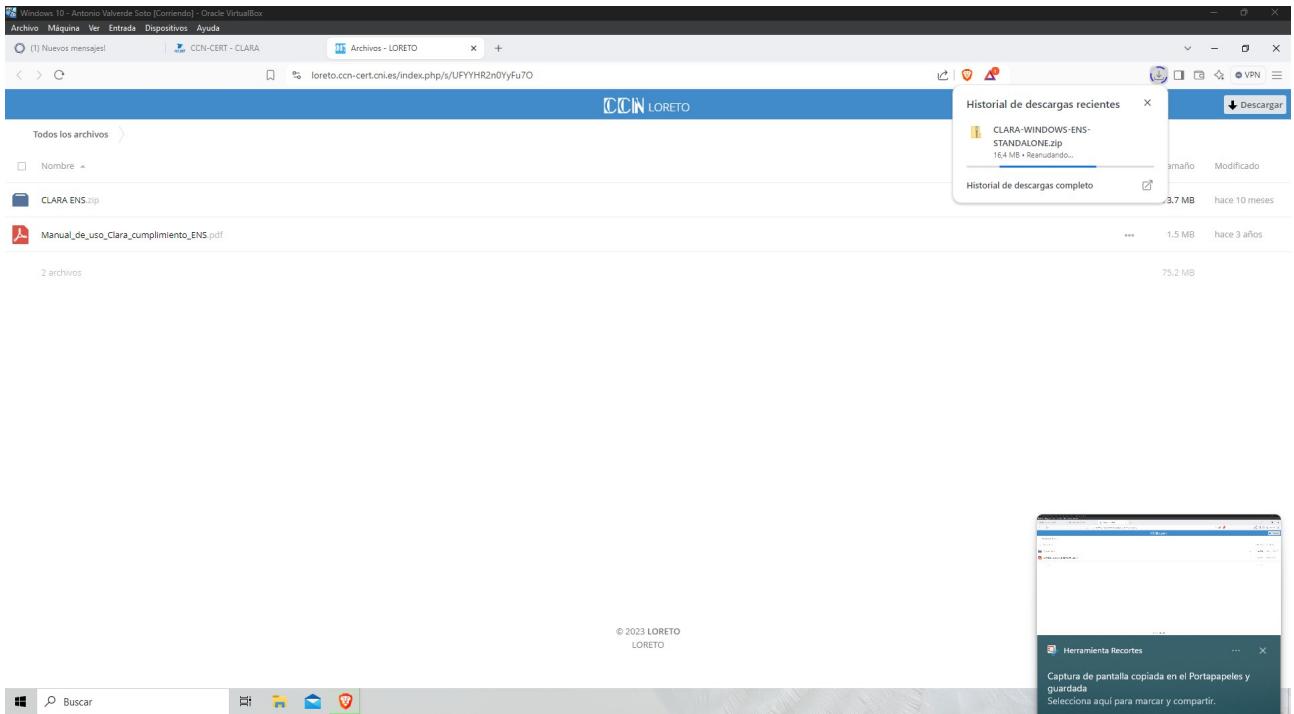
CLARA ENS Linux [\[Descarga\]](#) Contraseña: CLARA | Firma SHA [\[Descarga\]](#)

Contacto: clara@ccn-cert.cni.es

Clave PGP [Descargar](#)

FINGERPRINT 396D 3BA4 871E 97D0 0FB4 5466 BB28 1290 602B 0386

Ahora procedo a instalar la aplicación Clara en Windows, pinchando en Descarga.



Todos los archivos >

Nombre ▾

CLARA ENS.zip

Manual_de_uso_Clara_cumplimiento_ENS.pdf

2 archivos

Historial de descargas recientes

CLARA-WINDOWS-ENS-STANDALONE.zip
16.4 MB + Reiniciando...

Historial de descargas completo

3.7 MB hace 10 meses

1.5 MB hace 3 años

75.2 MB

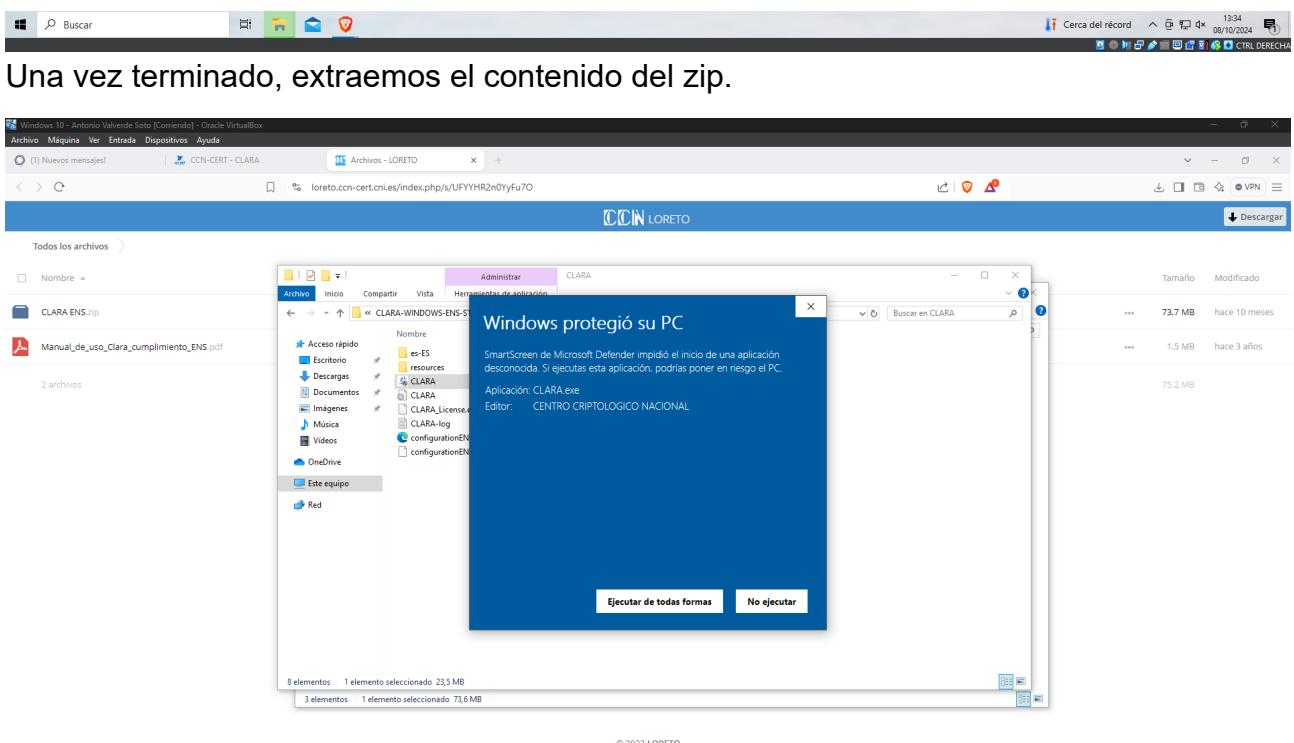
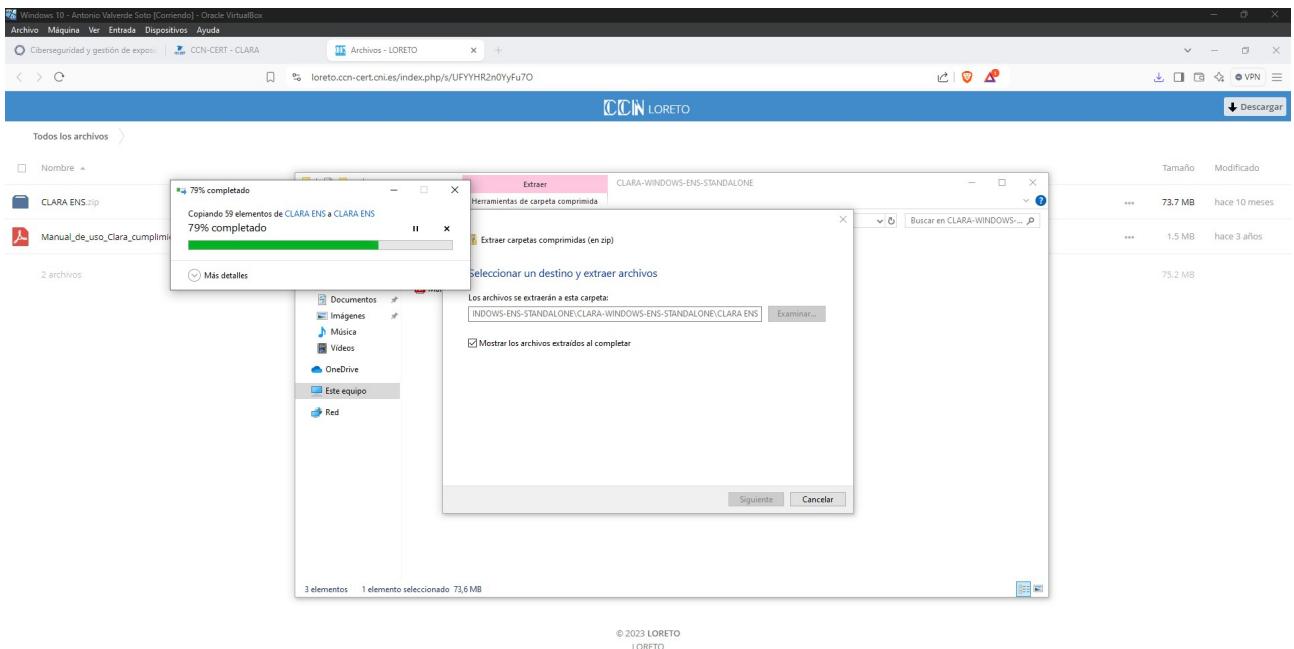
© 2023 LORETO

Herramienta Recortes

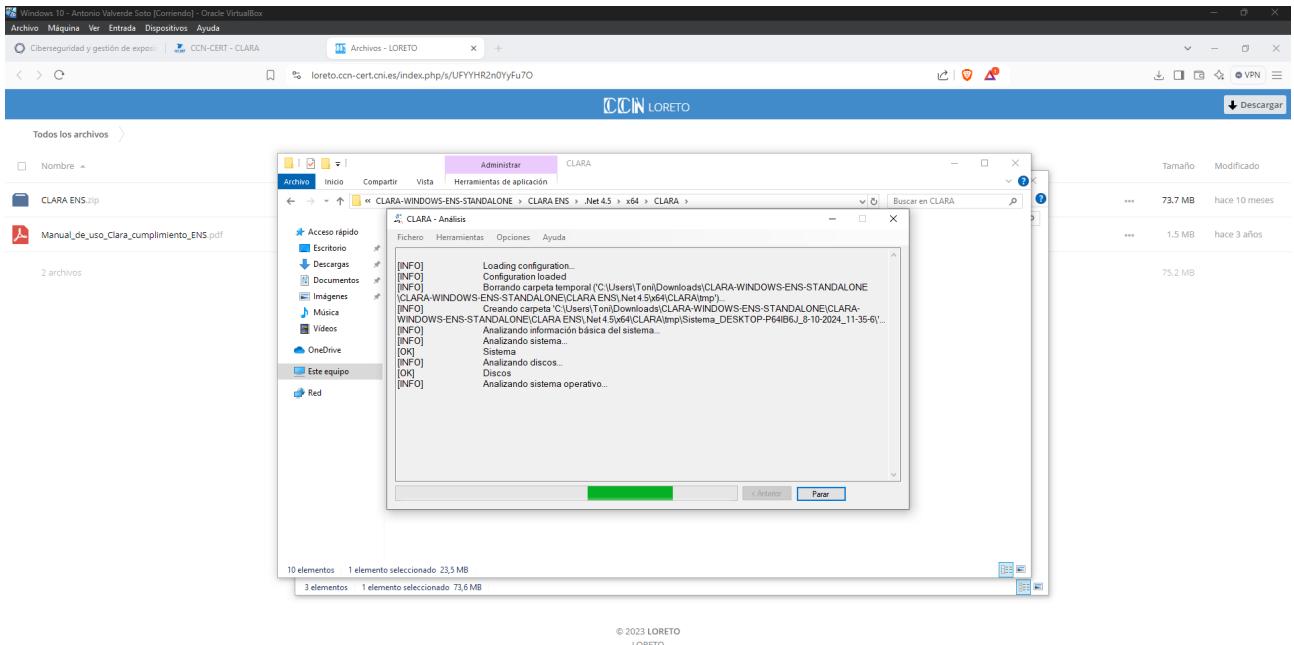
Captura de pantalla copiada en el Portapapeles y guardada

Selección aquí para marcar y compartir.

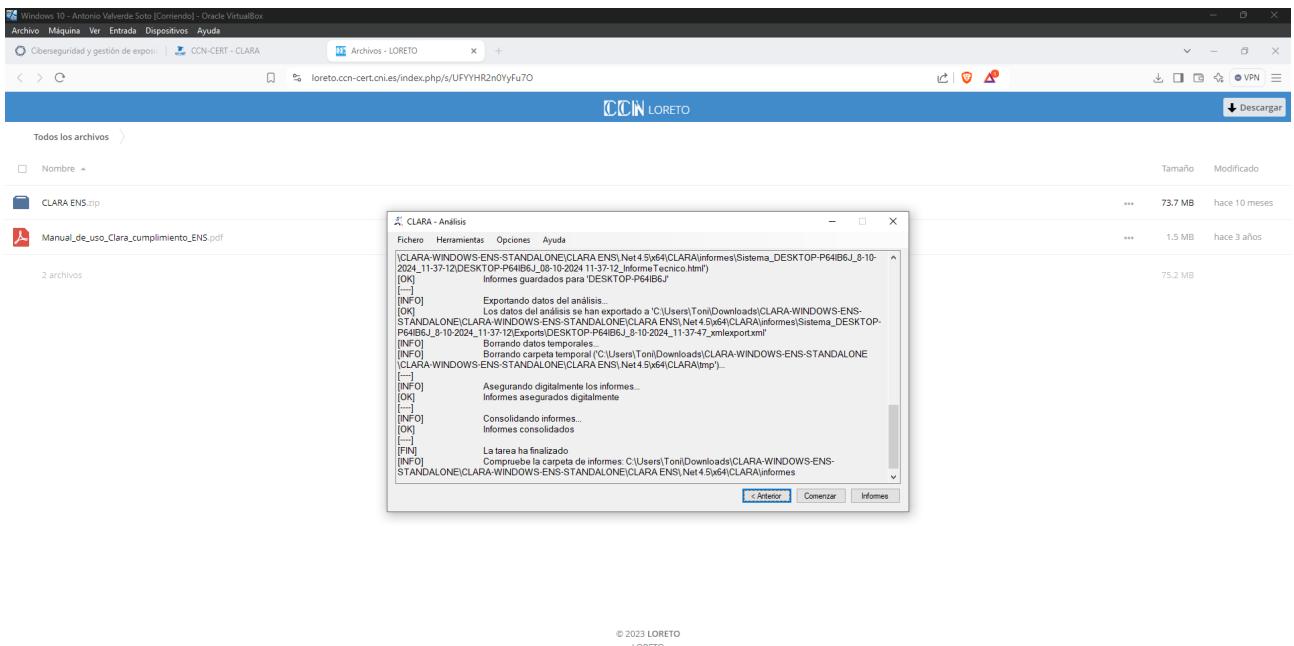
Nos lleva a este enlace, y pulsamos en descargar, automáticamente se nos descarga un zip.



Ejecutamos el programa Clara.



Una vez iniciado arrancamos la auditoría.

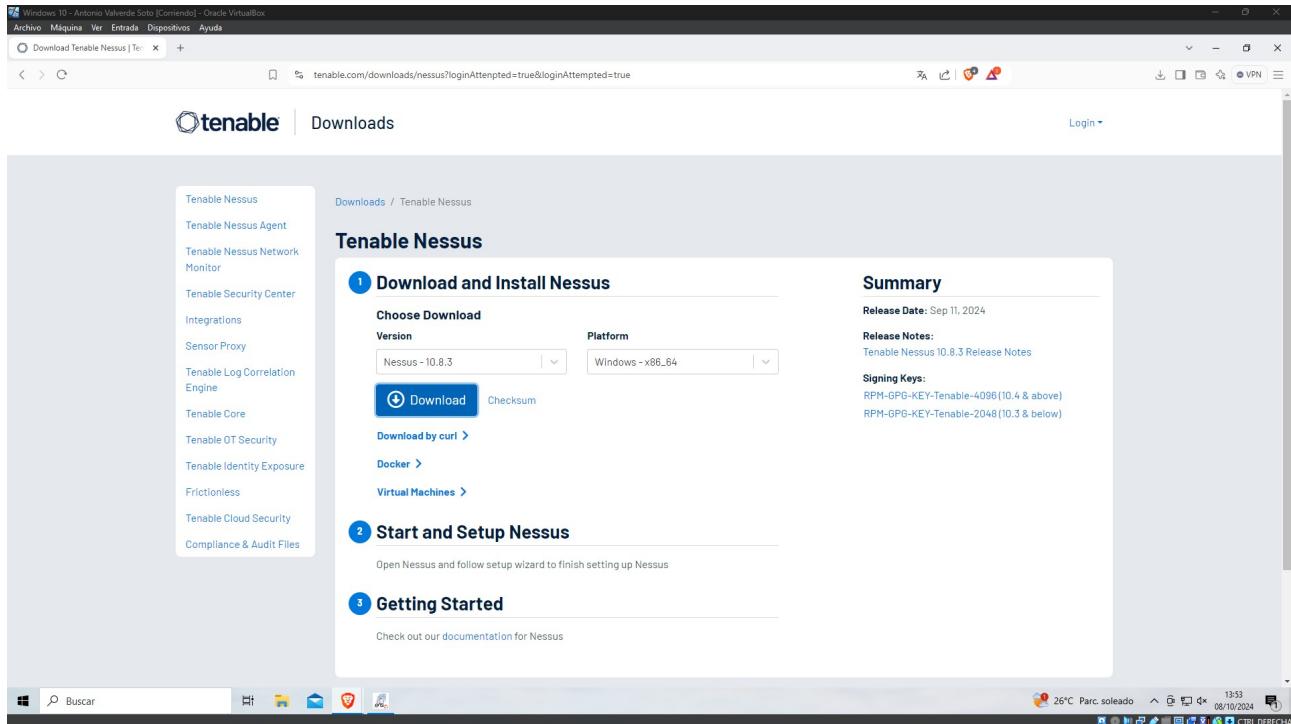


Una vez terminado, copio el resultado y lo pego en un fichero llamado Auditoría-Clara.txt.

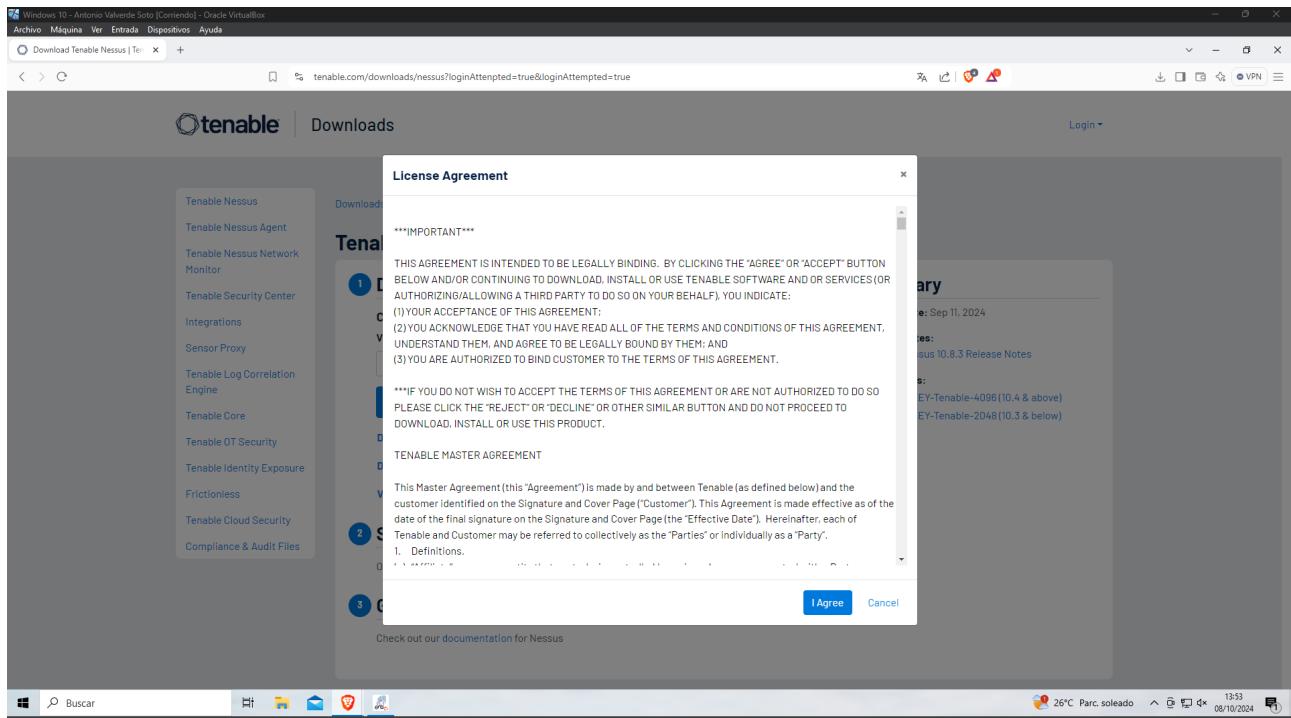
En este enlace muestro la auditoría de clara.

Ejercicio 3

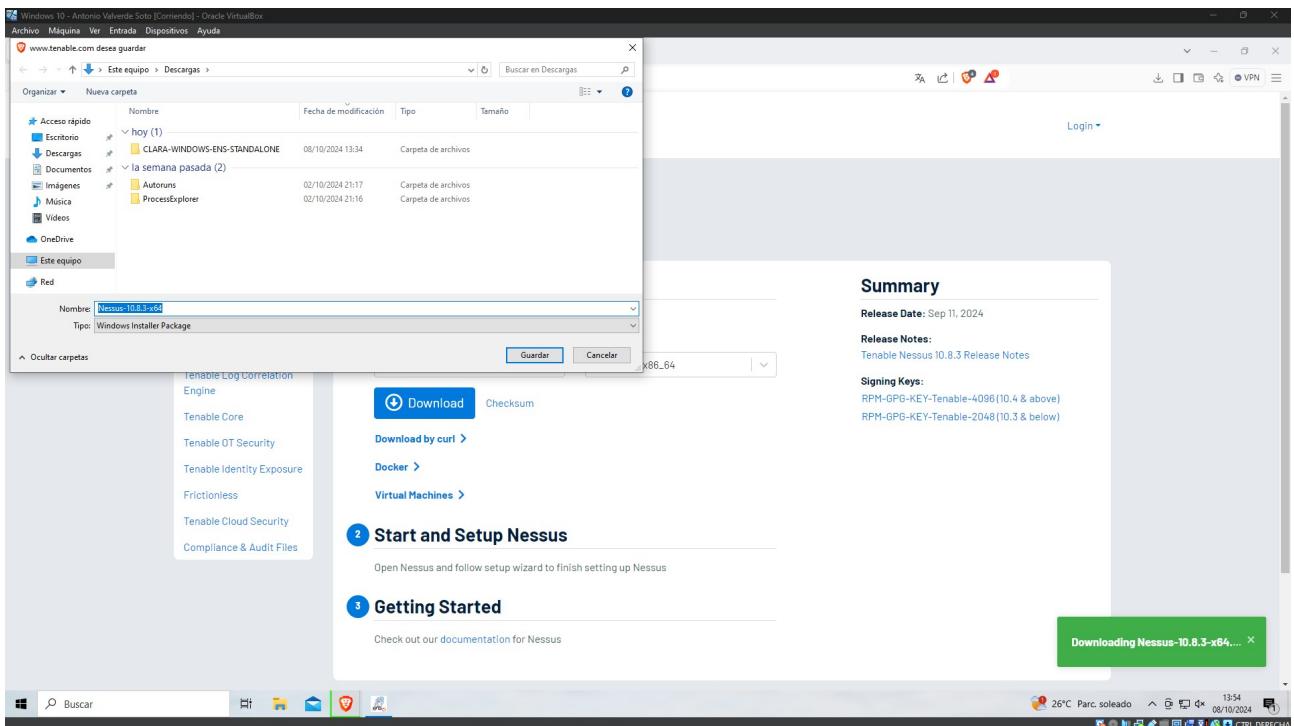
Nessus en Windows



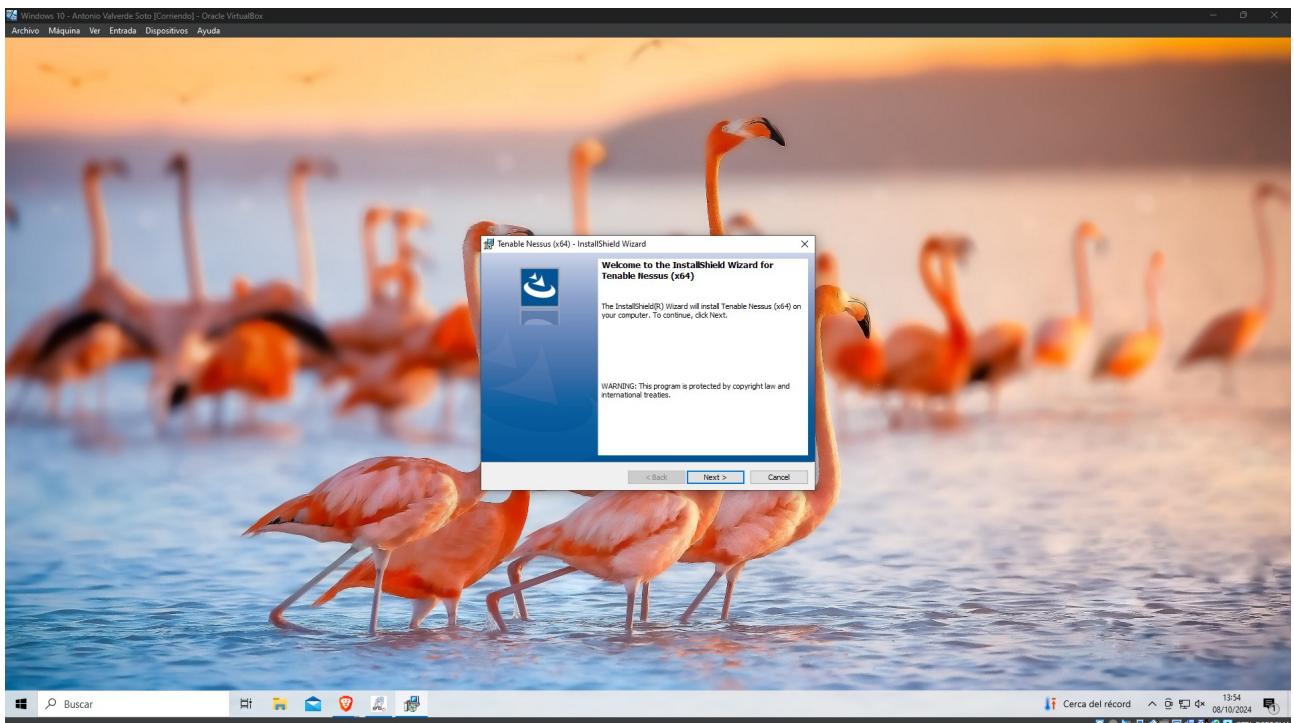
Entramos en las descargas de Tenable y descargamos Nessus para Windows.



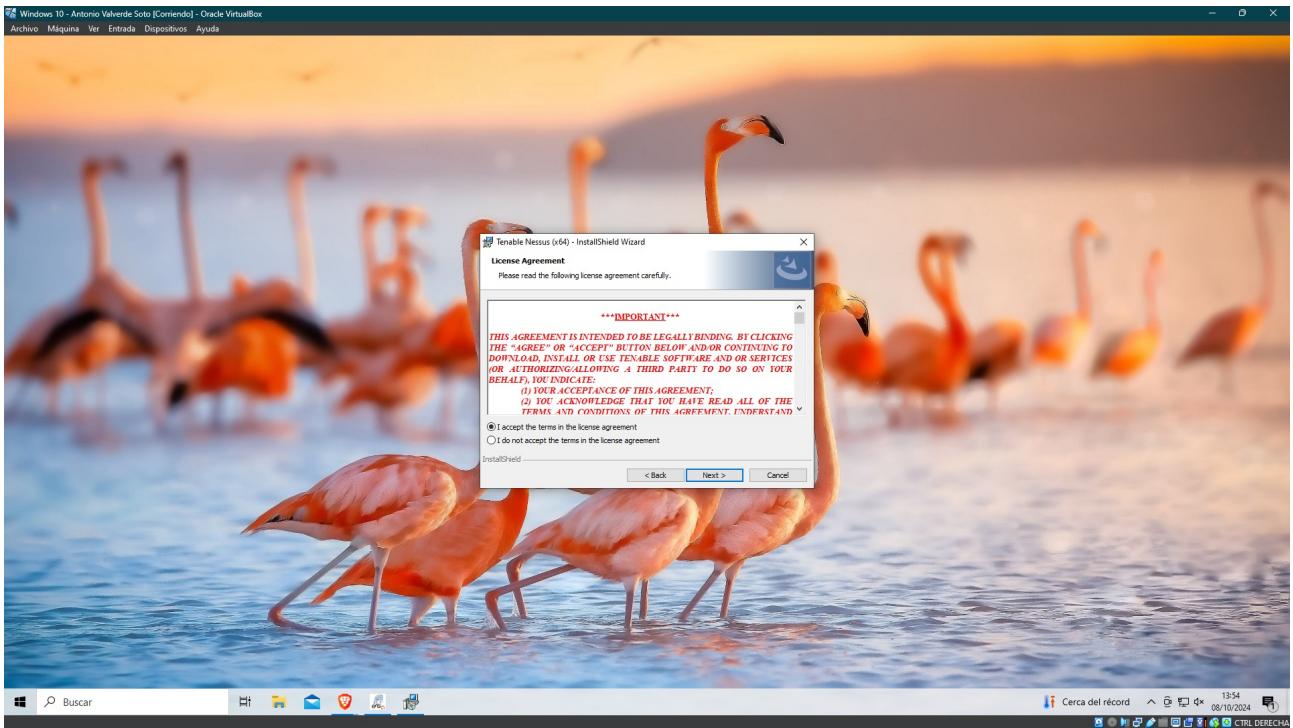
Al hacer click en descargar nos manda este mensaje de licencia.



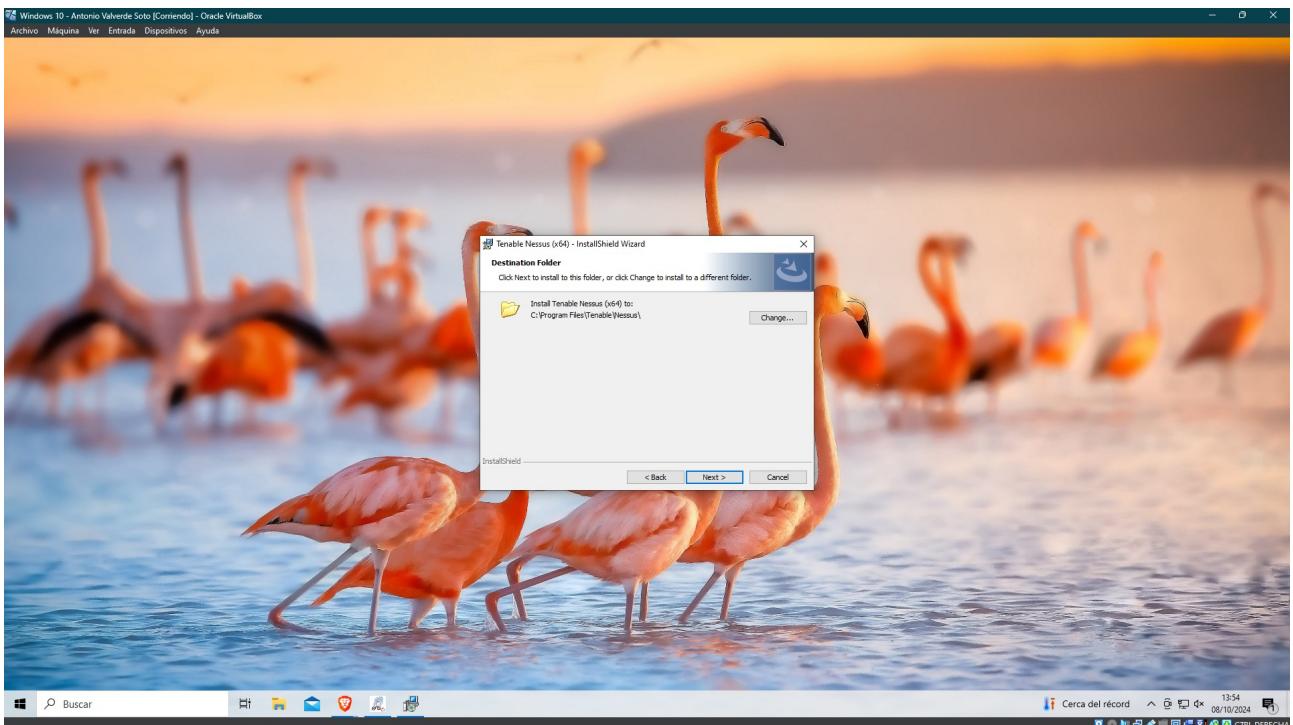
Indicamos la carpeta a la que vamos a enviar el ejecutable de la descarga.



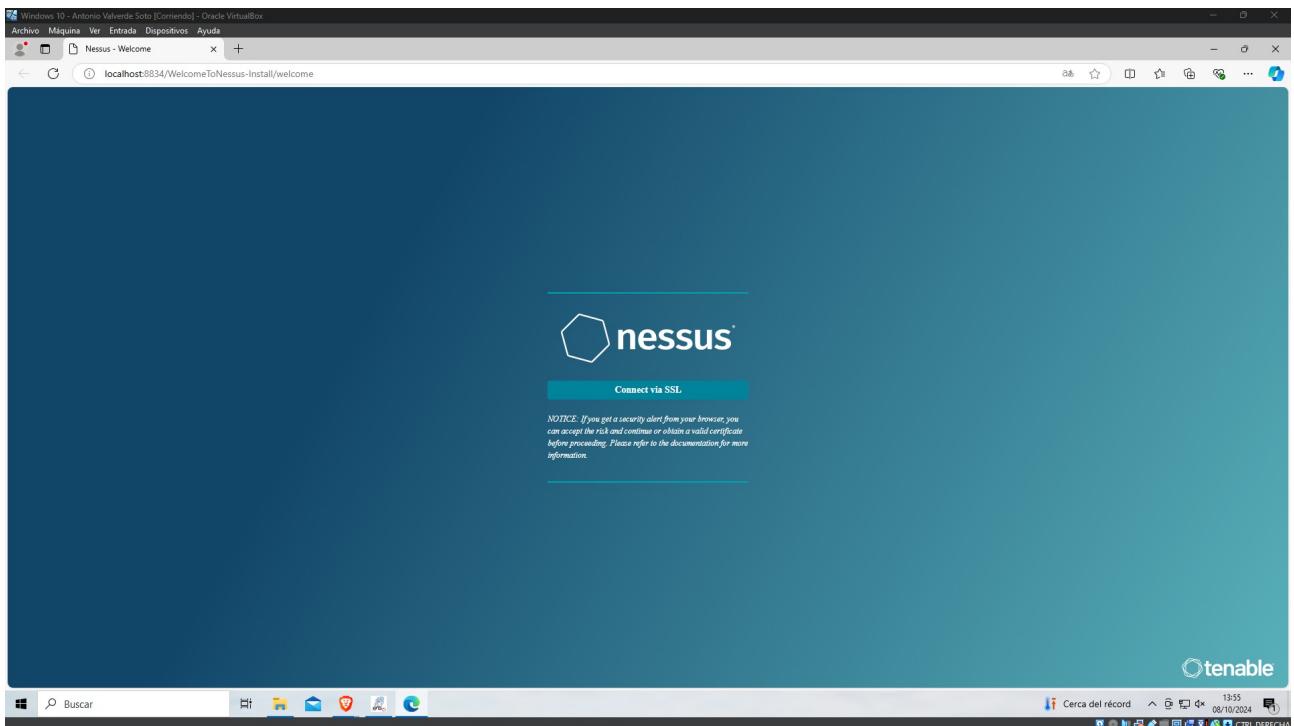
Una vez abierto nos muestra esta primera pantalla.



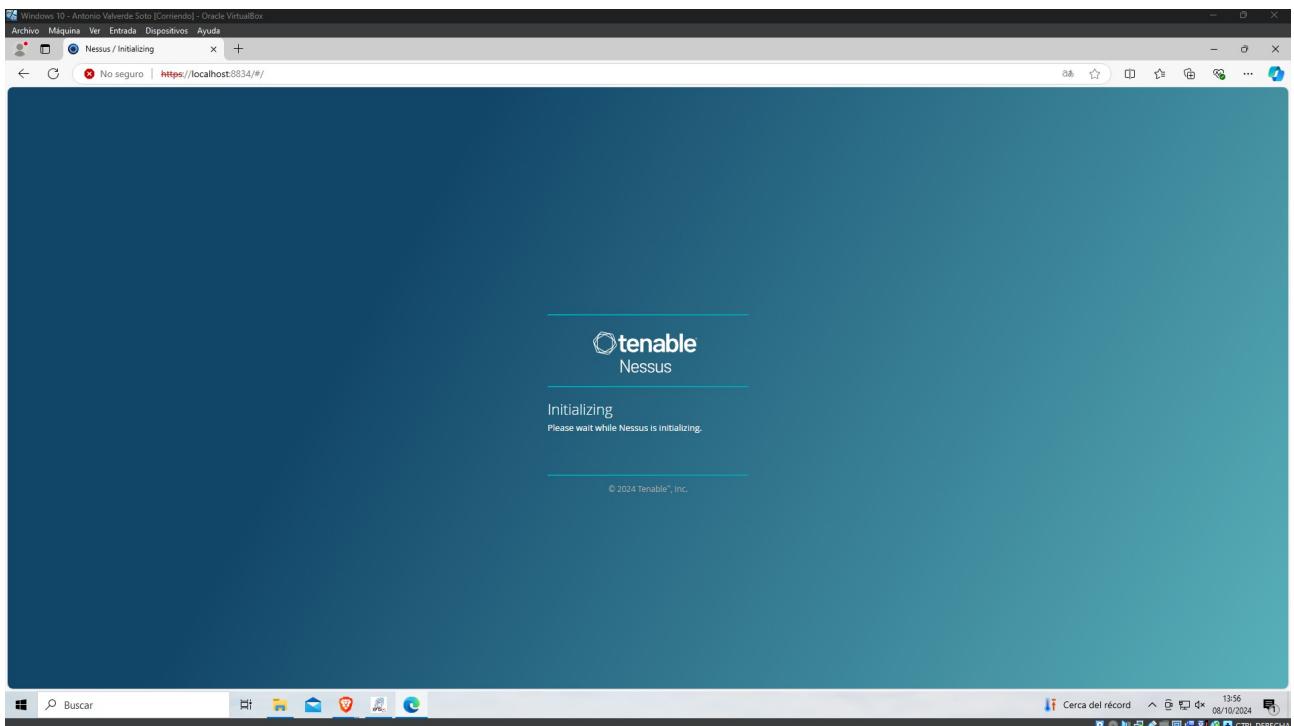
Aceptamos los términos de licencia y continuamos con el siguiente paso.



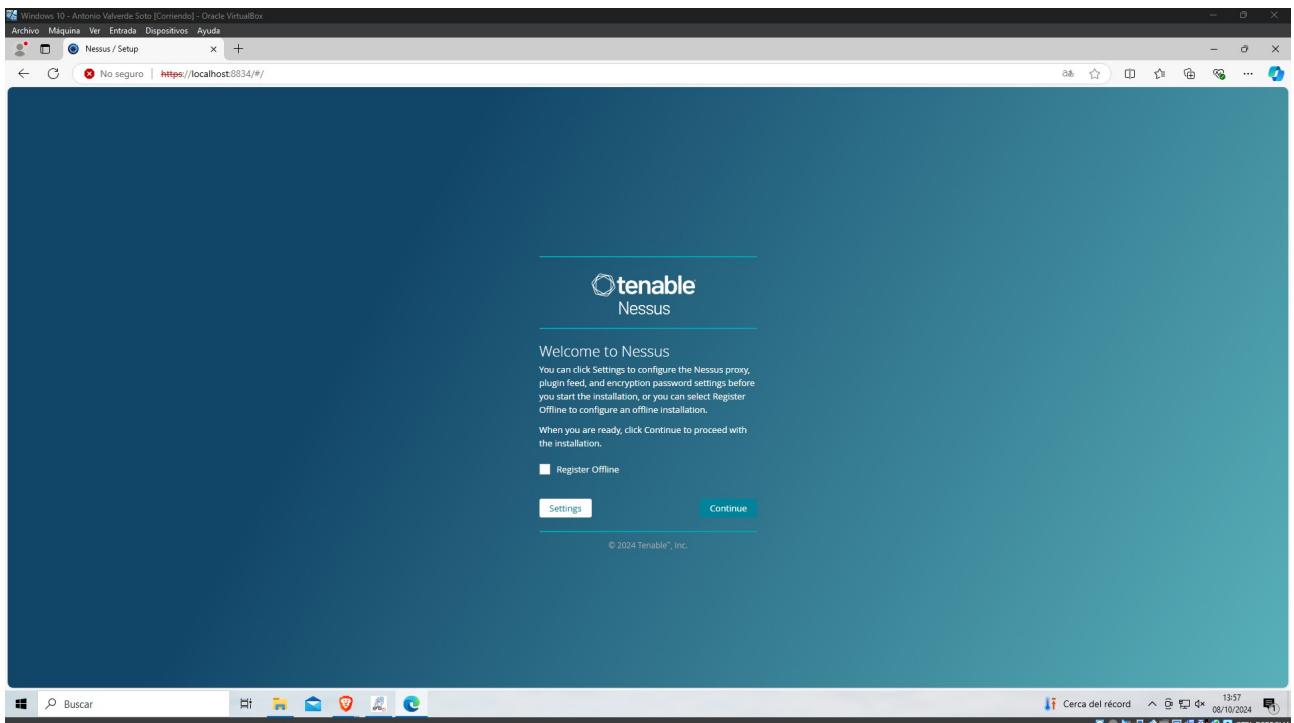
Elegimos el fichero en el que se va a guardar Nessus.



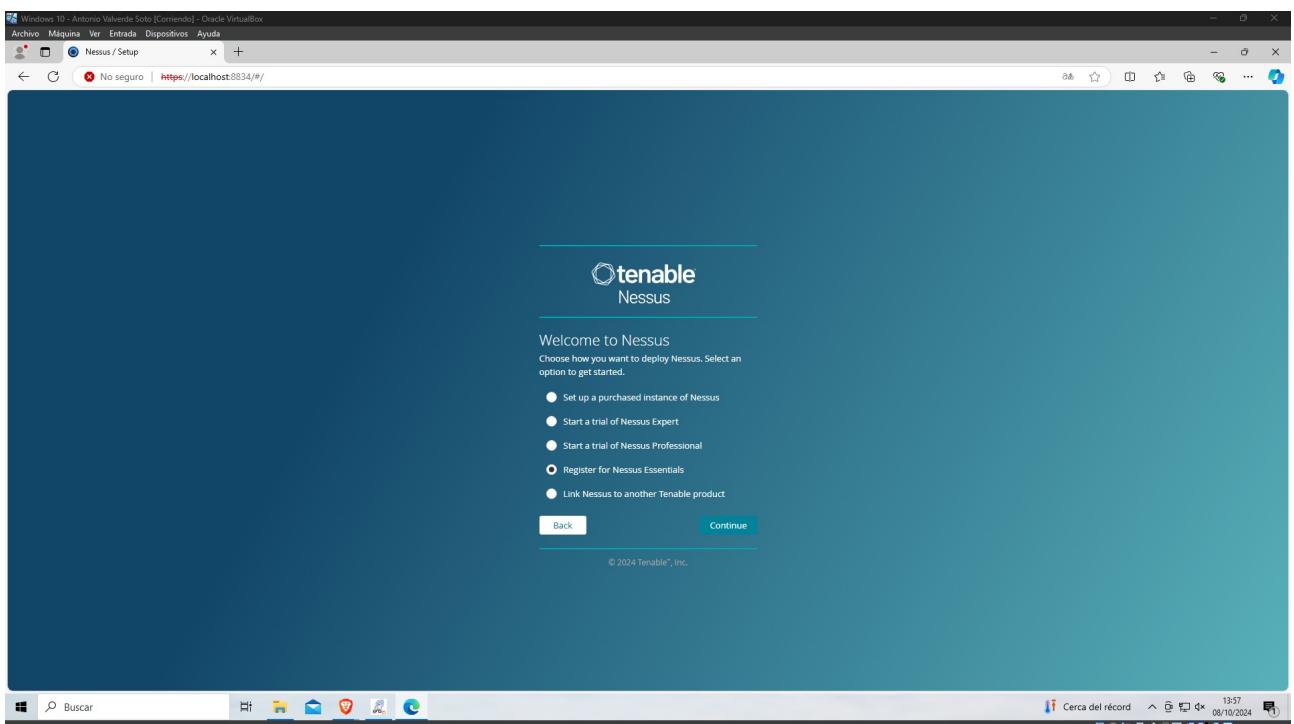
Una vez terminado se arranca el servidor nessus y se nos abre esta enlace en la web. Ejecutándose en localhost y con el puerto 8834, que es el puerto por defecto de nessus.



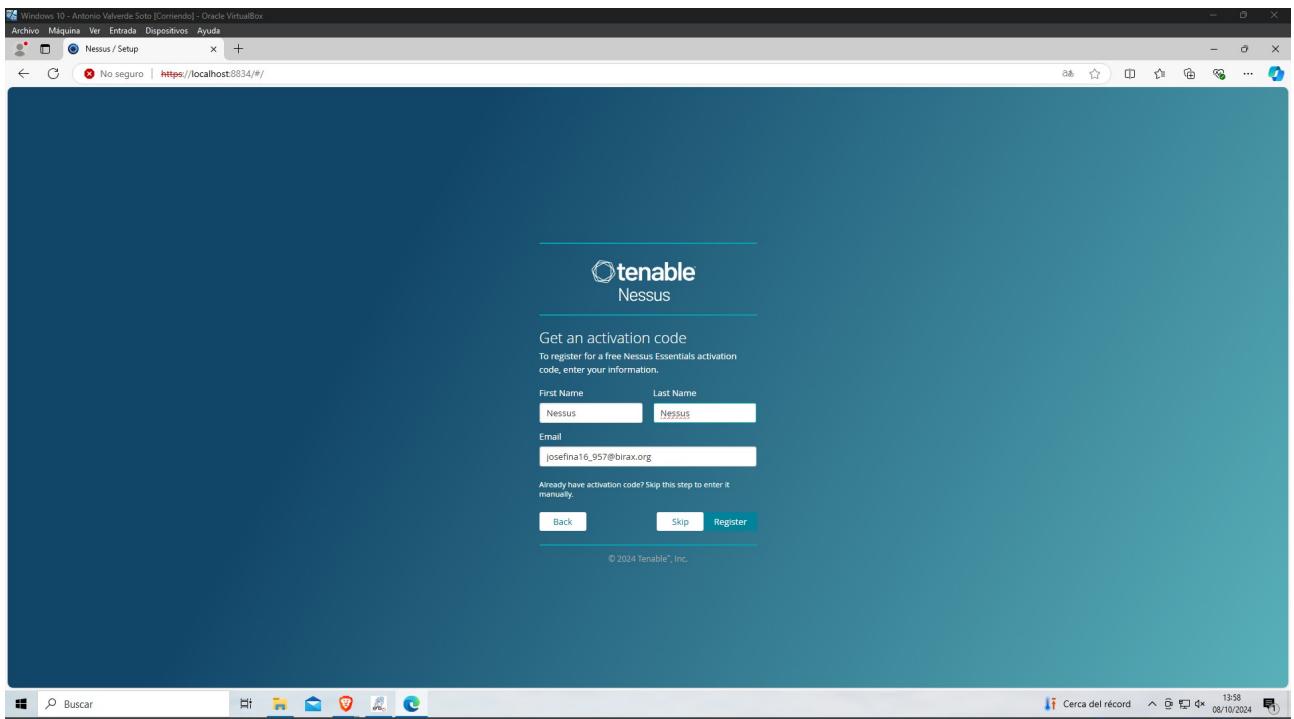
Una vez que le damos a conectar se inicia el proceso.



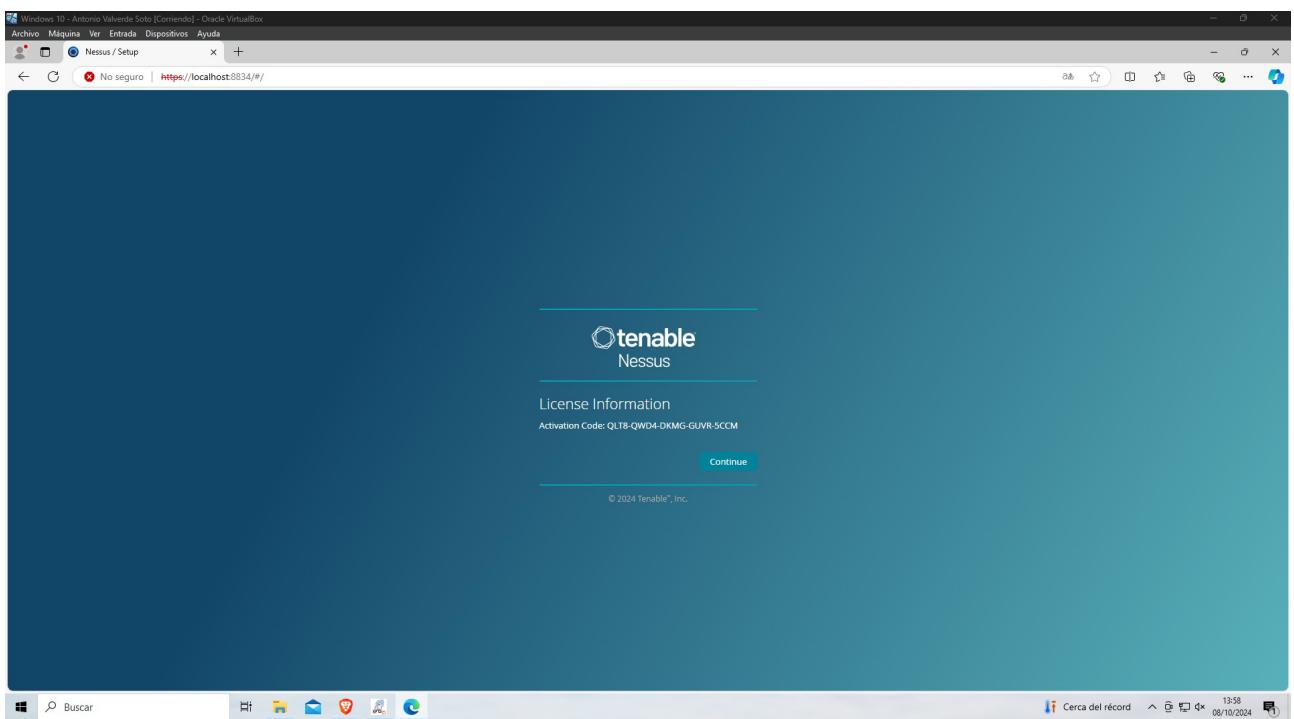
Esta es la primera pestaña que nos sale, sirve para registrarnos.



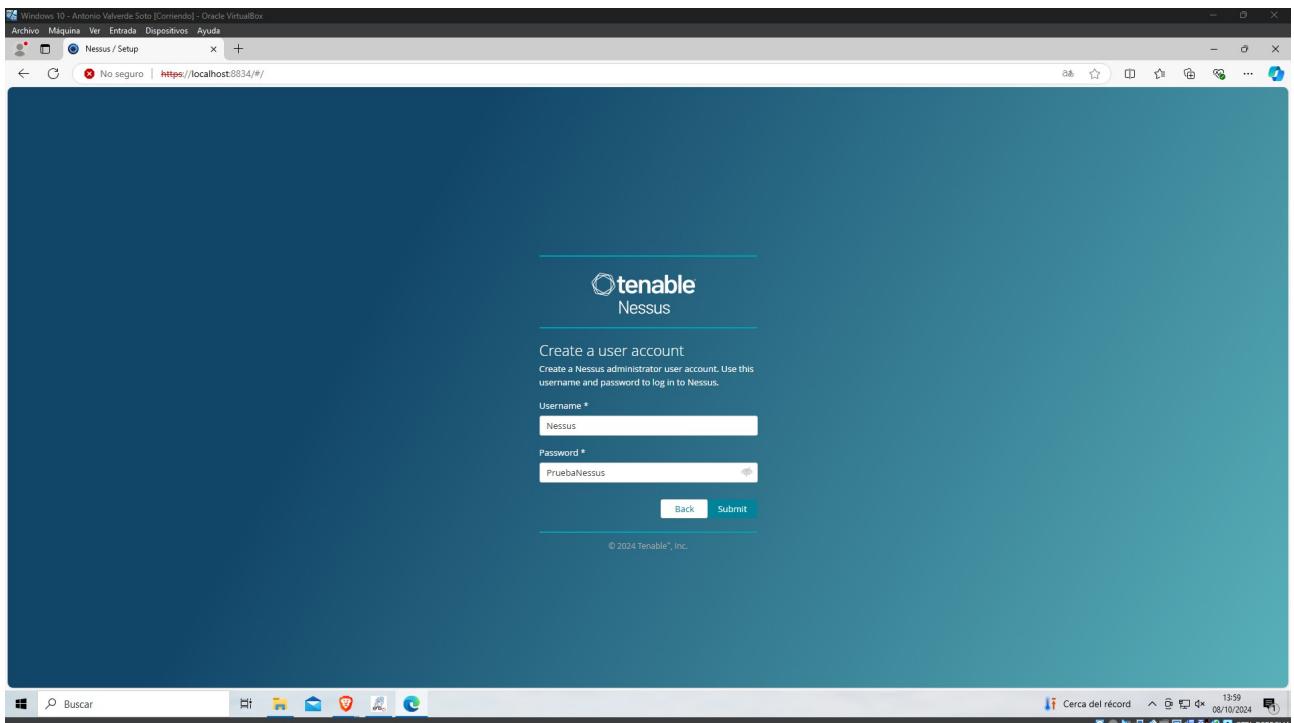
Elijo la opción de registrarme en Nessus Essentials.



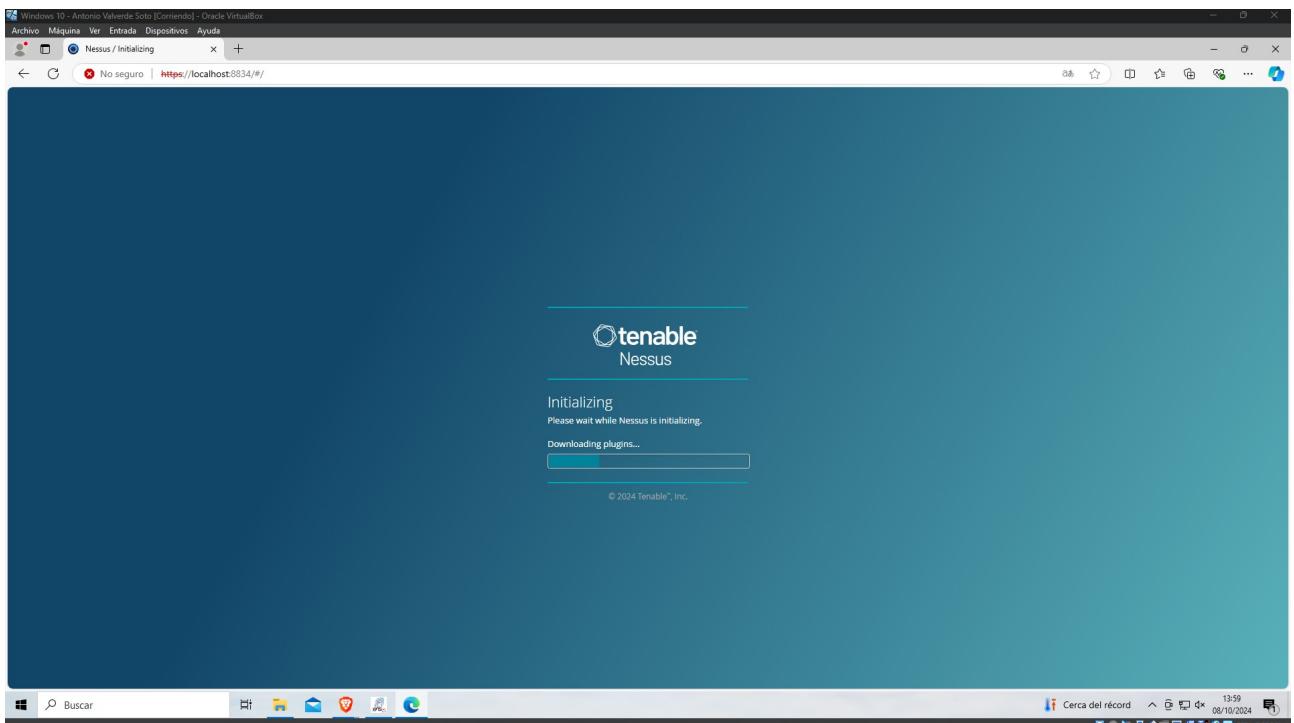
Indico el nombre y el correo, he usado un correo temporal para este proceso.



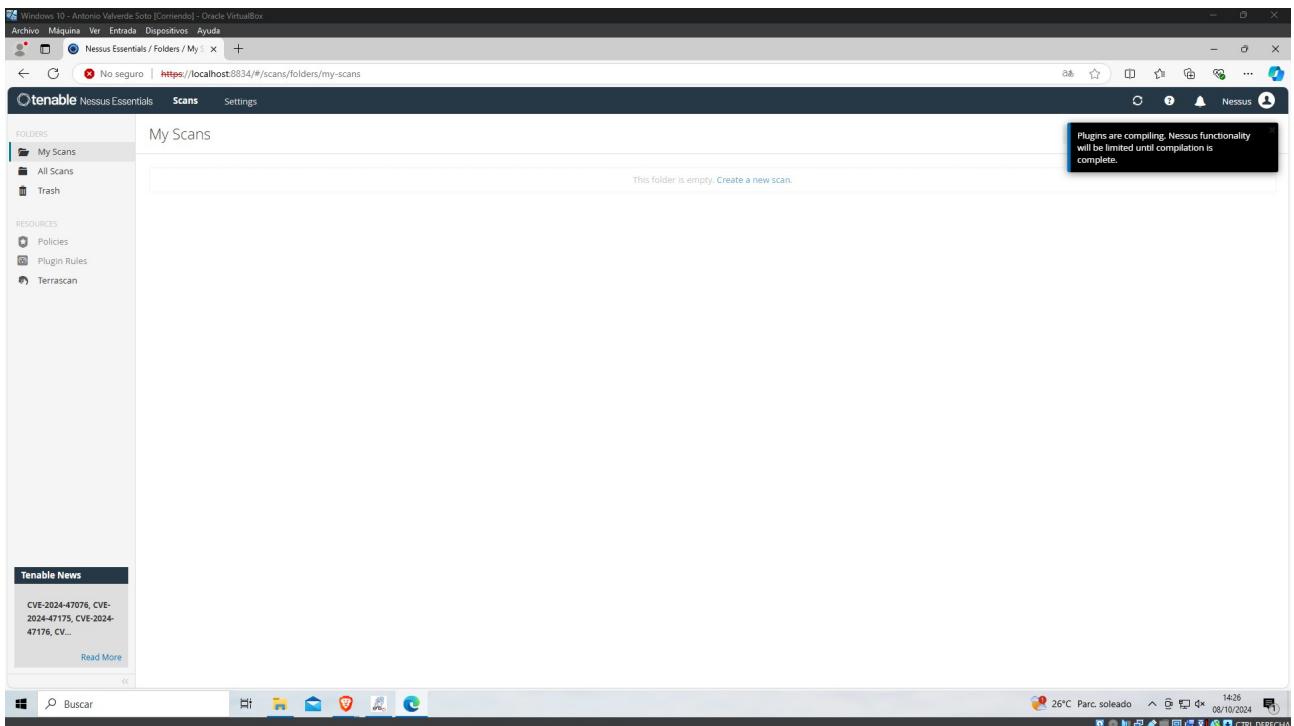
Aquí me indica el código de activación de la licencia.



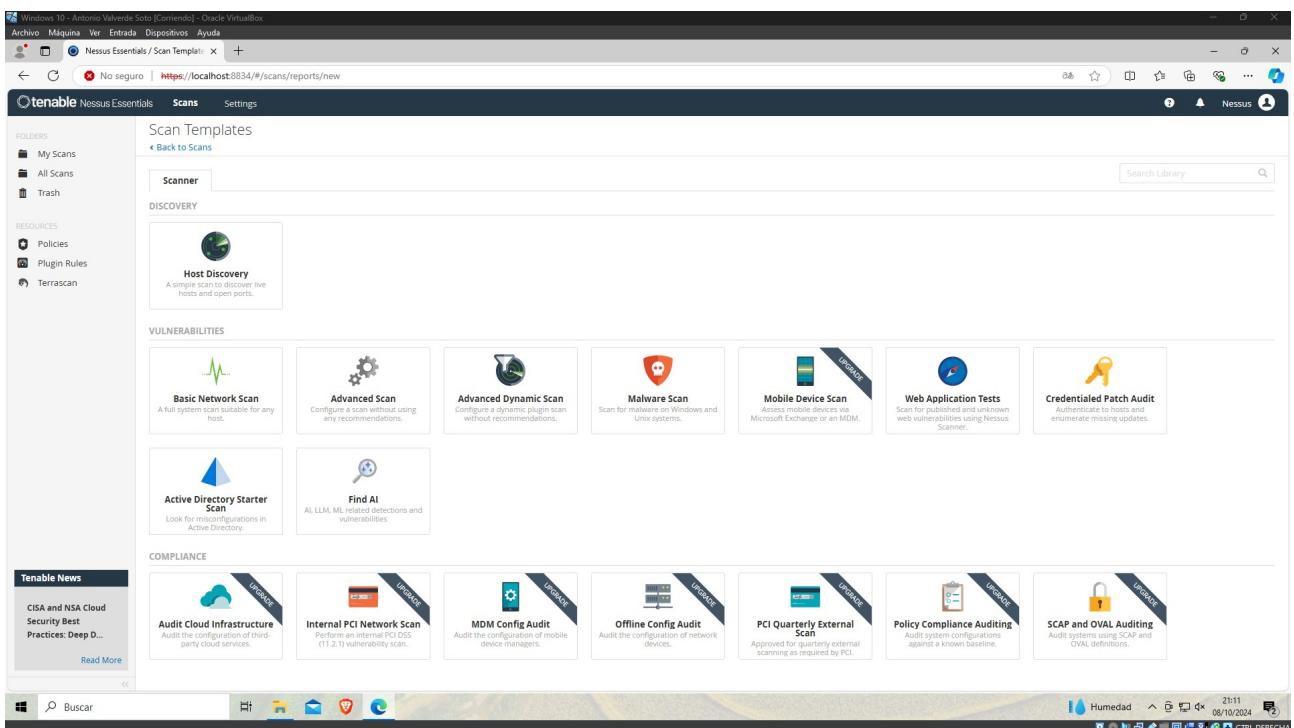
Ahora indico el nombre de usuario y la contraseña. Al ser para una actividad, no he puesto una contraseña segura.



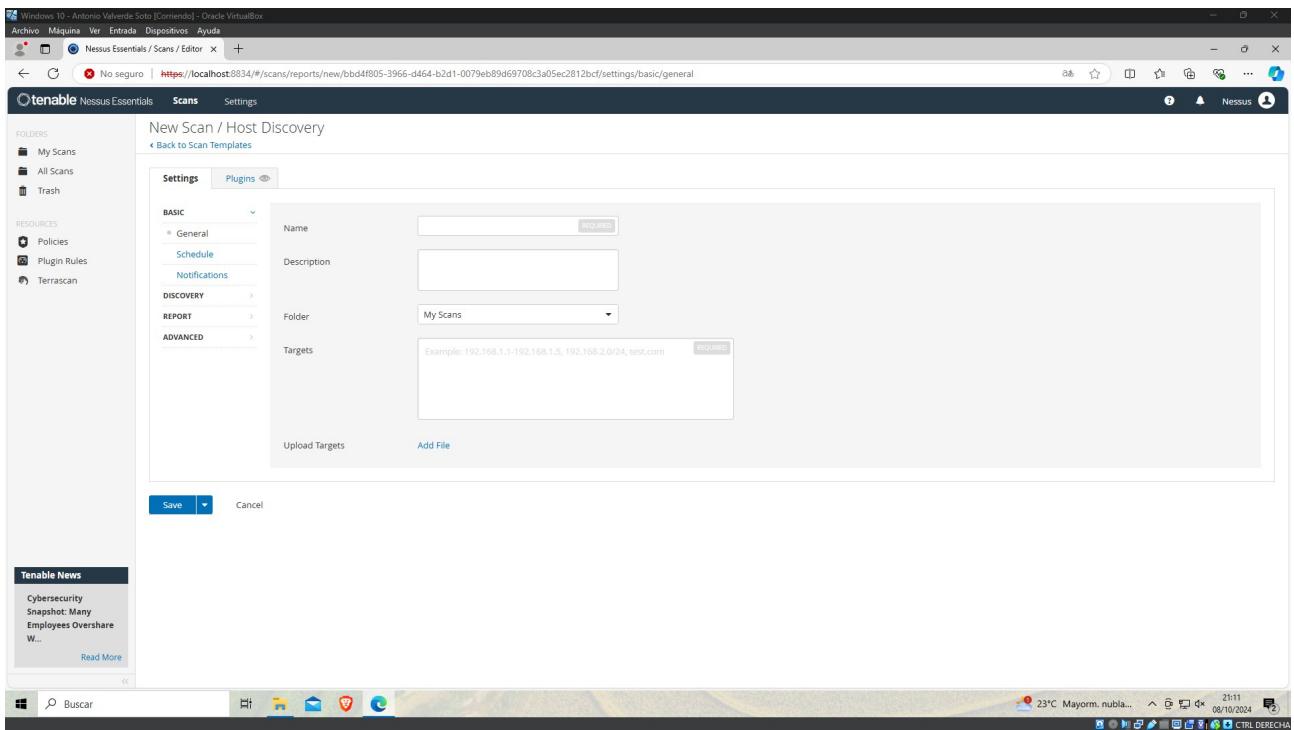
Ahora inicia el proceso de instalación de los pluggins.



Al terminar el proceso se nos abre este menú. Y tenemos que esperar a que termine el proceso de compilación de los pluggins.



Una vez terminado, dándole a New Scan, podemos elegir el tipo de escaneo que queremos hacer.



Elegimos un nombre, una descripción en caso de que queramos, escribimos una descripción y en el sector de targets, elegimos el rango que queremos escanear.

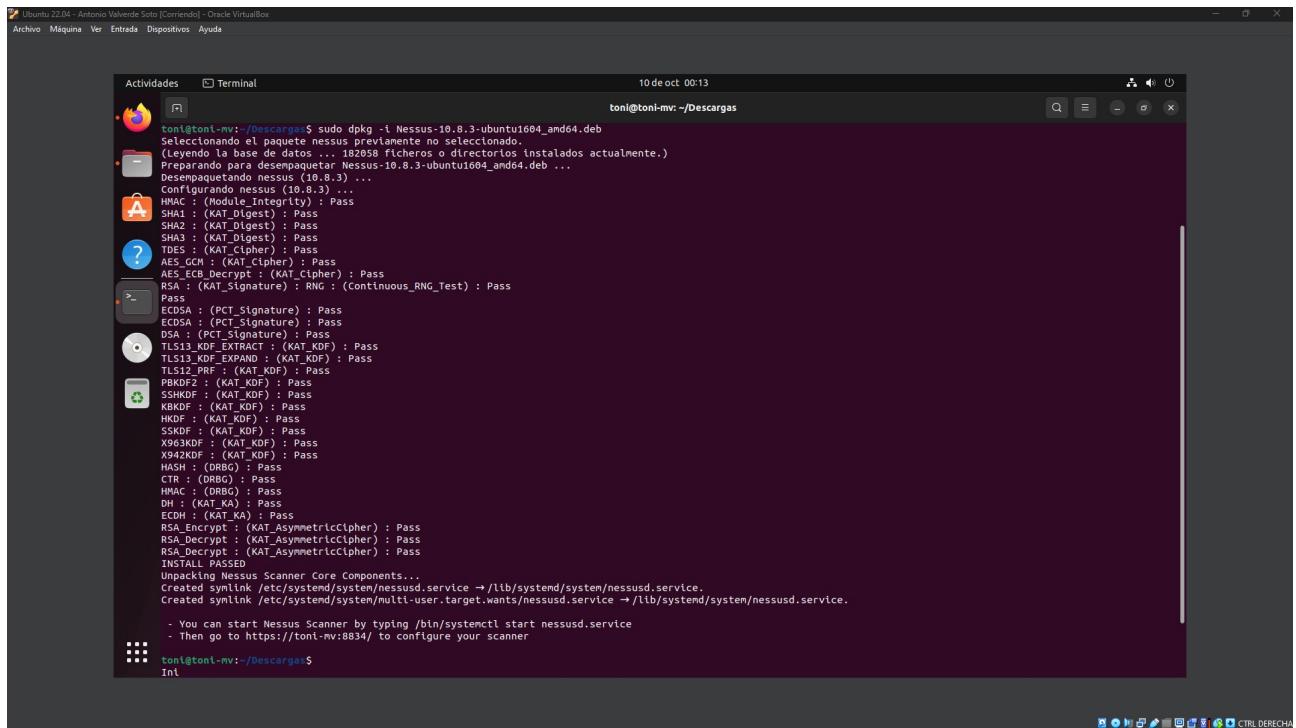
En mi caso, tengo dos redes en mi casa, y realizo un escaneo de ambas, desde la 192.168.0.1 a la 192.168.0.254, y de la 192.168.68.1 a la 192.168.68.254. Lo indico exactamente de la siguiente forma: 192.168.0.1-192.168.0.254, 192.168.68.1-192.168.68.254.

Al terminar, nos muestra diferentes cosas, y le damos a Report, de esa forma se nos crea un pdf que muestra la siguiente Auditoría.

[Pulsa aquí para ver la auditoría de Nessus en Windows.](#)

Nessus en Linux

Una vez en Linux, entramos en el mismo enlace, que anteriormente y descargamos Nessus, esta vez eligiendo la opción de Ubuntu.

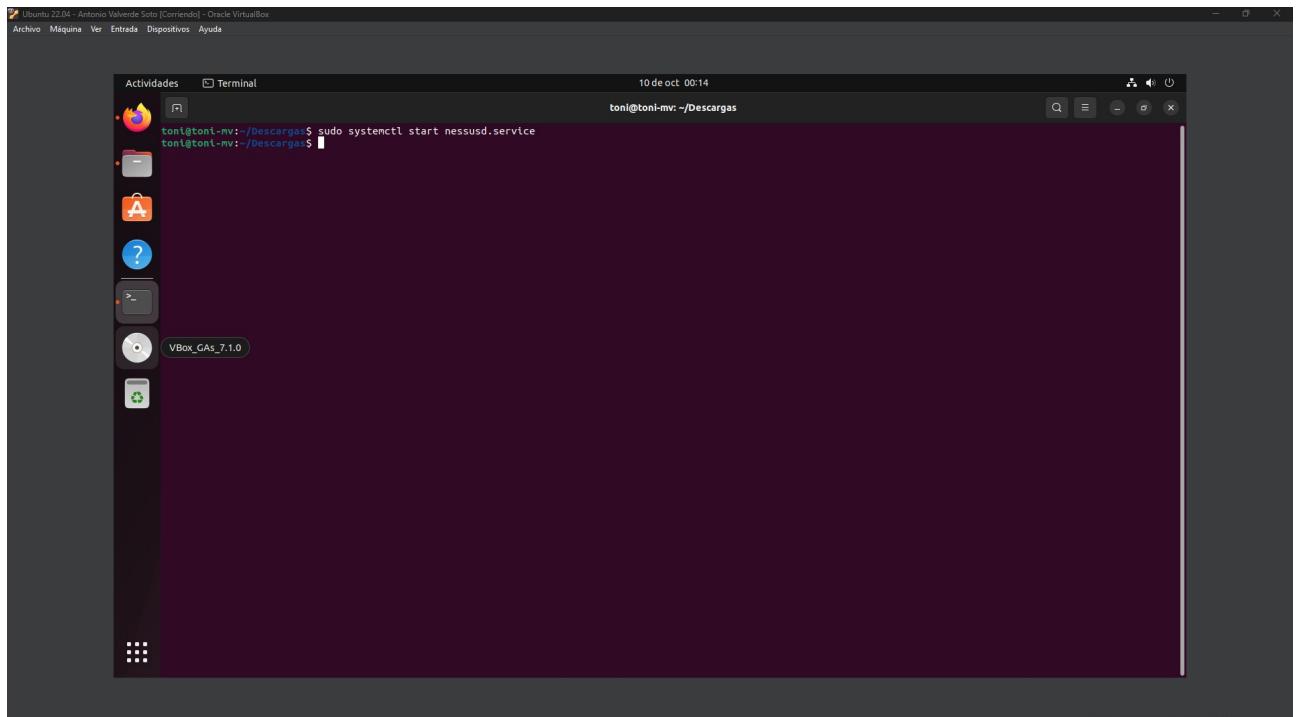


```
Ubuntu 22.04 - Antonio Valverde Soto [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal 10 de oct 00:13
toni@toni-mv: ~/Descargas
toni@toni-mv:~/Descargas$ sudo dpkg -i Nessus-10.8.3-ubuntu1604_amd64.deb
Selecctionando el paquete nessus previamente no seleccionado.
(Leer descripción del paquete... 182058 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar nessus-10.8.3-ubuntu1604_amd64.deb ...
Desempaquetando nessus (10.8.3) ...
Configurando nessus (10.8.3) ...
HMAC : (Module Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SM3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDH : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_PRF : (KAT_KDF) : Pass
PBKDF : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
RHKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMW : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_Asymmetriccipher) : Pass
RSA_Decrypt : (KAT_Asymmetriccipher) : Pass
RSA_Decrypt : (KAT_Asymmetriccipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...
Created symlink /etc/systemd/system/nessusd.service → /lib/systemd/system/nessusd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/nessusd.service → /lib/systemd/system/nessusd.service.

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://toni-mv:8834/ to configure your scanner
toni@toni-mv:~/Descargas$ int
```

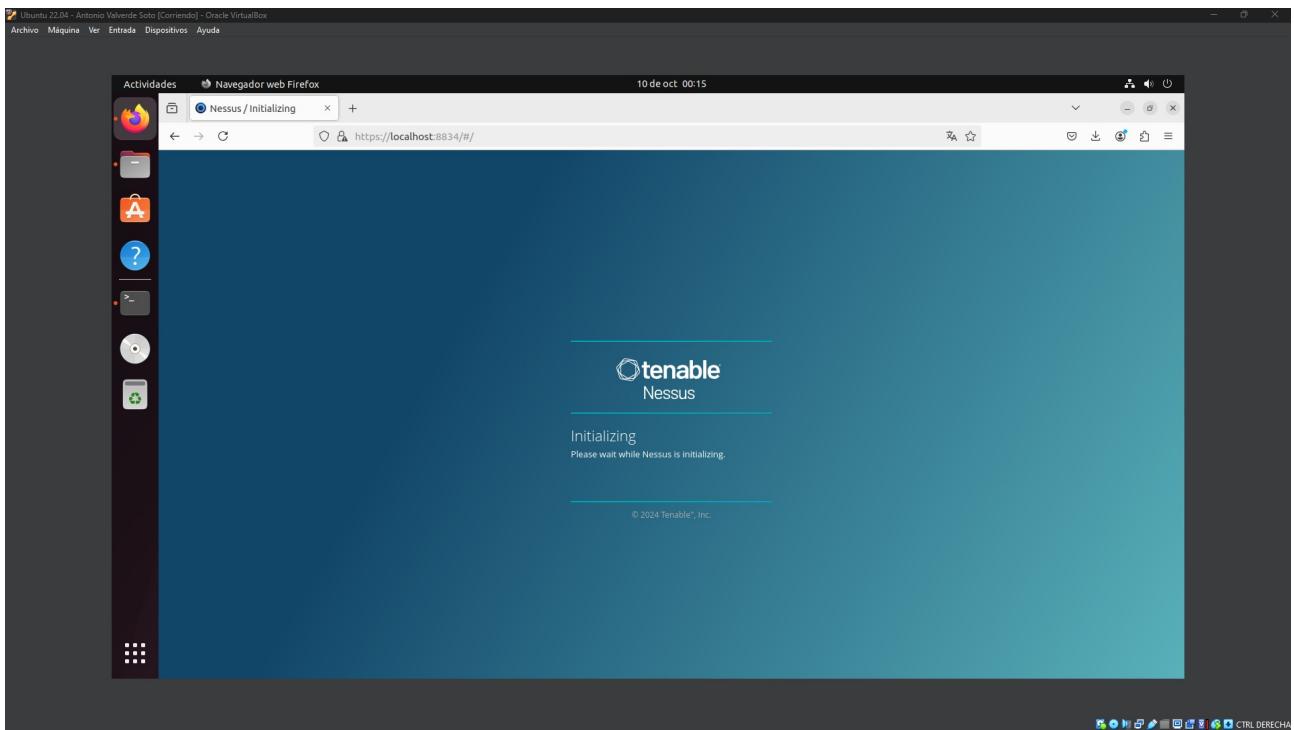
Se nos descarga un fichero.deb, con el comando sudo dpkg -i y la ruta del fichero se nos descarga Nessus, y realimos los mismos pasos que previamente en Windows.



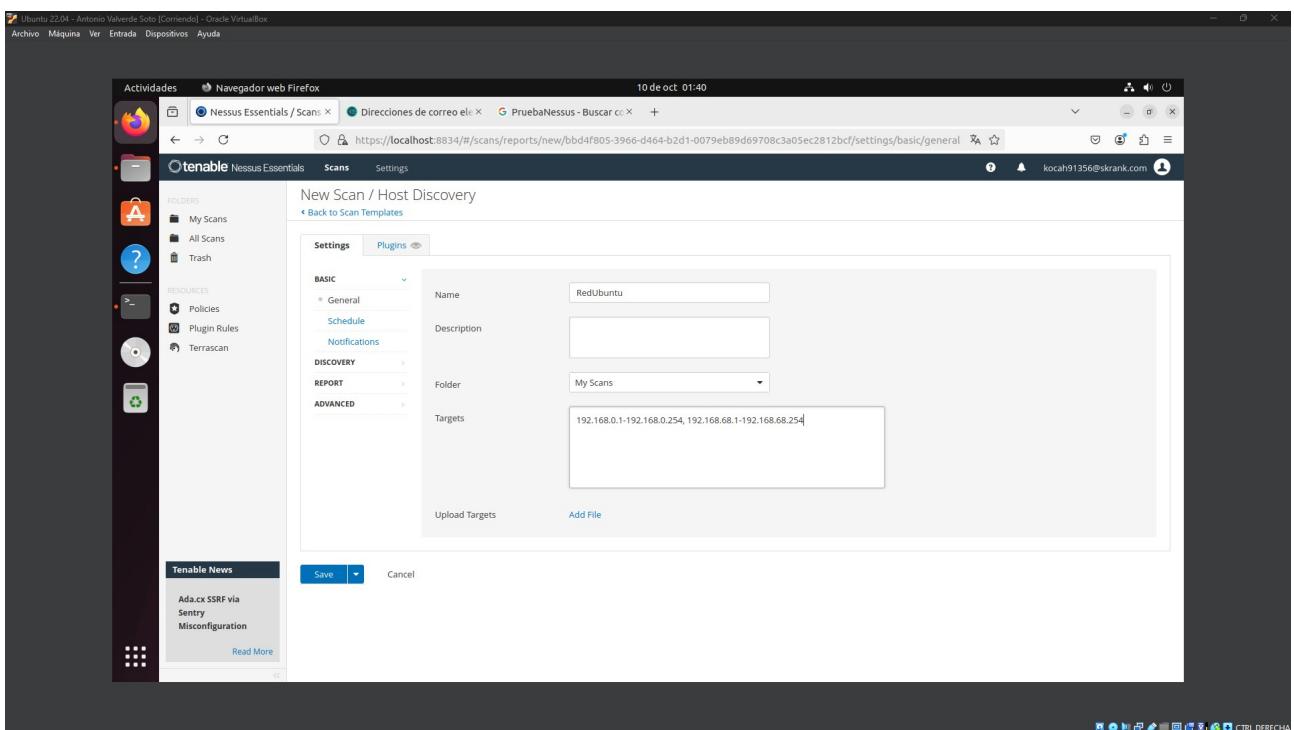
```
Ubuntu 22.04 - Antonio Valverde Soto [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal 10 de oct 00:14
toni@toni-mv: ~/Descargas$ sudo systemctl start nessusd.service
toni@toni-mv:~/Descargas$
```

Tenemos que arrancar el servicio de Nessus manualmente para poder entrar en el enlace, igual que he hecho antes en Windows.



Entramos en <https://localhost:8834>, lo tenemos que introducir manualmente.



Hacemos lo mismo que hemos hecho antes en Windows, ya que el proceso de pluggins es igual que el anterior hecho en Windows.

Aquí hago una auditoría de la red igual que antes.

[En este enlace está la Auditoría de Nessus en Linux.](#)